

ARAGONESA DE SERVICIOS TELEMÁTICOS

Instalación Componente Cliente

Manual de usuario

Referencia:	AST-EFIRMA-InstalacionComponenteCliente.doc
Autor:	Aragonesa de Servicios Telemáticos
Fecha de creación:	05/11/2014
Última actualización:	05/11/2014
Versión:	1.6
Clasificación:	Uso Público



Contenido

Entidad Pública Aragonesa de Servicios Telemáticos
Pº María Agustín 25-27-29 • 50071 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4395
www.aragon.es

1. Componente Cliente

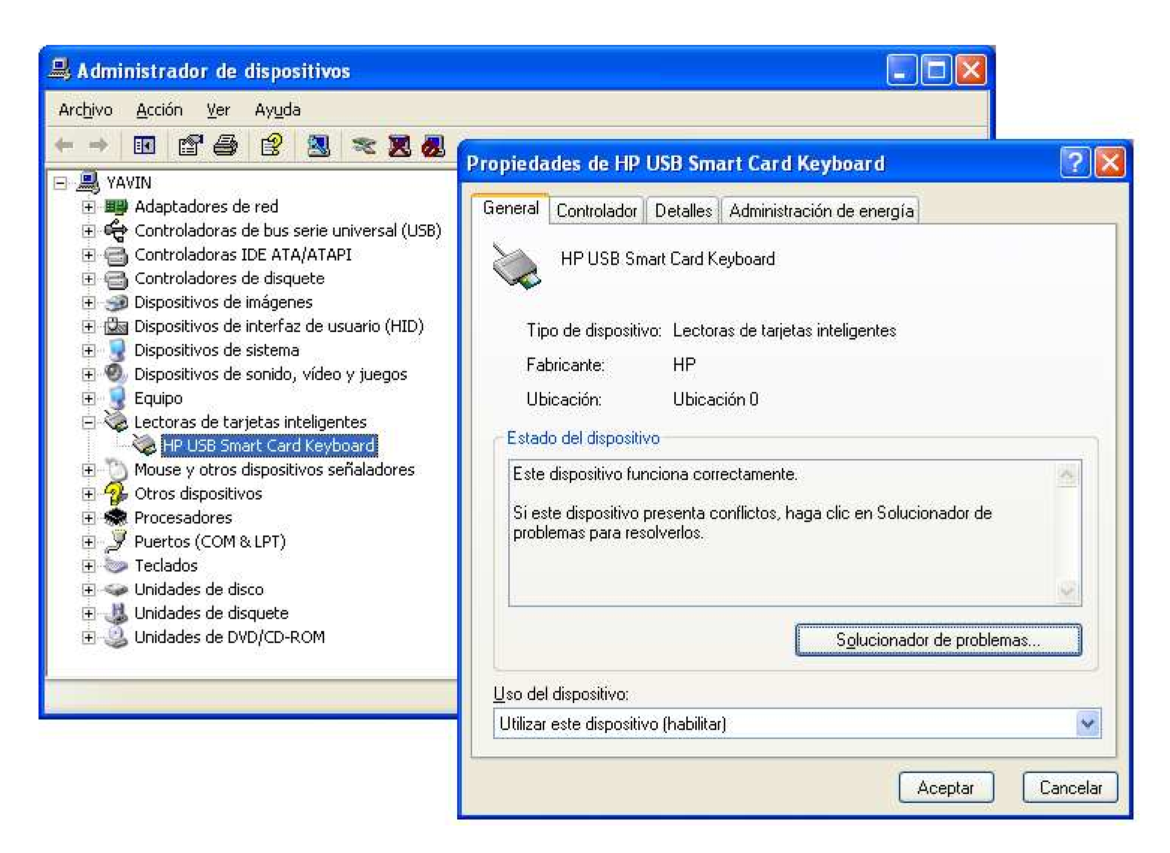
El componente cliente de la Plataforma de Firma de Gobierno de Aragón permite a un usuario la firma y el cifrado de documentos electrónicos desde una aplicación web, pudiendo acceder a los almacenes locales de certificados de su ordenador.

1.1. Requisitos

Para la correcta utilización del componente cliente y de sus funcionalidades es necesario tener en cuenta cierto número de requisitos previos.

1.1.1. Lector criptográfico

Es necesario tener correctamente instalado el teclado con lector criptográfico y sus drivers.



Administrador de dispositivos de MS Windows XP

1.1.2. Tarjetas Criptográficas

Disponer de una tarjeta criptográfica y haber instalado sus drivers, que son distintos para cada tipo de tarjeta (**CERES**, **DNI Electrónico**…). Estos drivers deben instalarse tanto para el **MS**

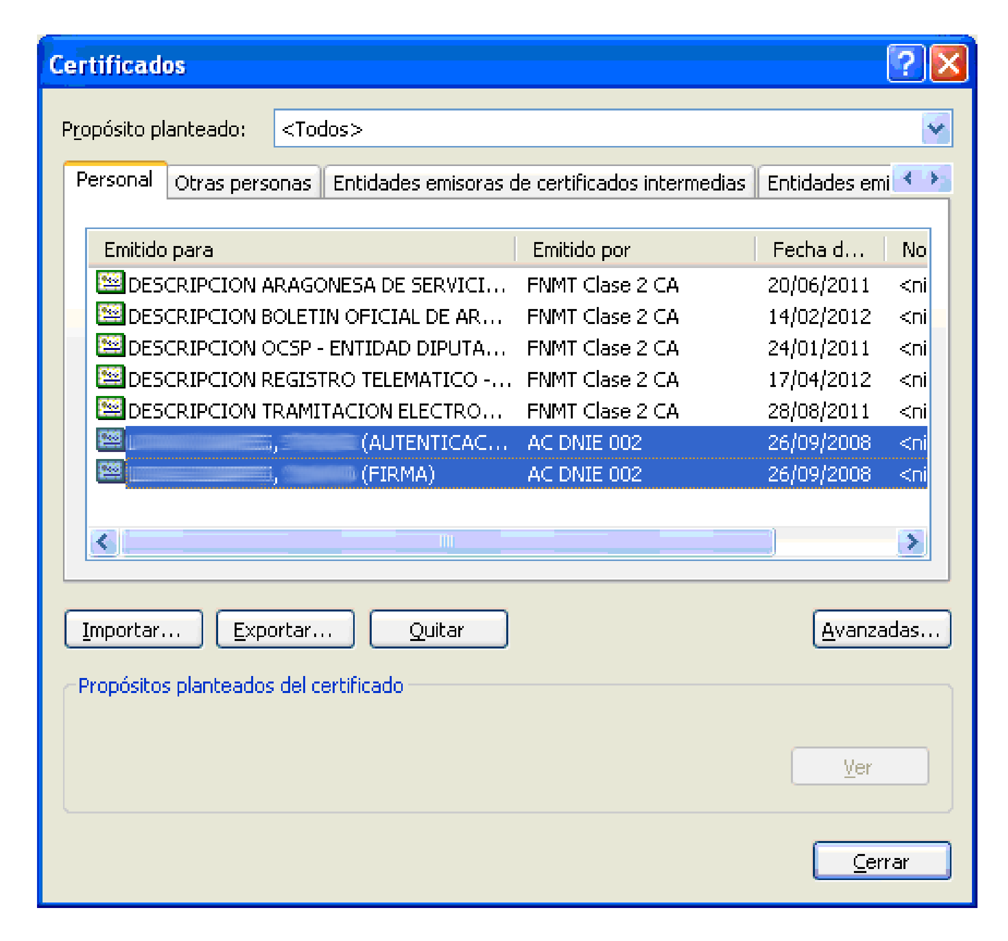
Certificate Store como para los diversos clientes que no usen el MS Certificate Store y que puedan hacer uso de las tarjetas (**Firefox**, **Thunderbird**…).

Tarjetas mas comunes	URL de descarga de sus drivers
DNI Electrónico	http://www.dnielectronico.es
Tarjeta CERES	http://www.cert.fnmt.es

Los drivers de estas tarjetas son independientes de los certificados y claves privadas que contengan, ya que las tarjetas son solamente un contenedor. En el caso del **DNI Electrónico**, éste solamente contendrá los certificados y claves de firma y autenticación emitidos por la **Dirección General de la Policía**, mientras que en las tarjetas **CERES**, al poder escribirse en ellas, podrán contener todo tipo de certificados y claves, como las emitidas por **FNMT**, **Camerfirma**, **Firmaprofesional**, **Ancert**…

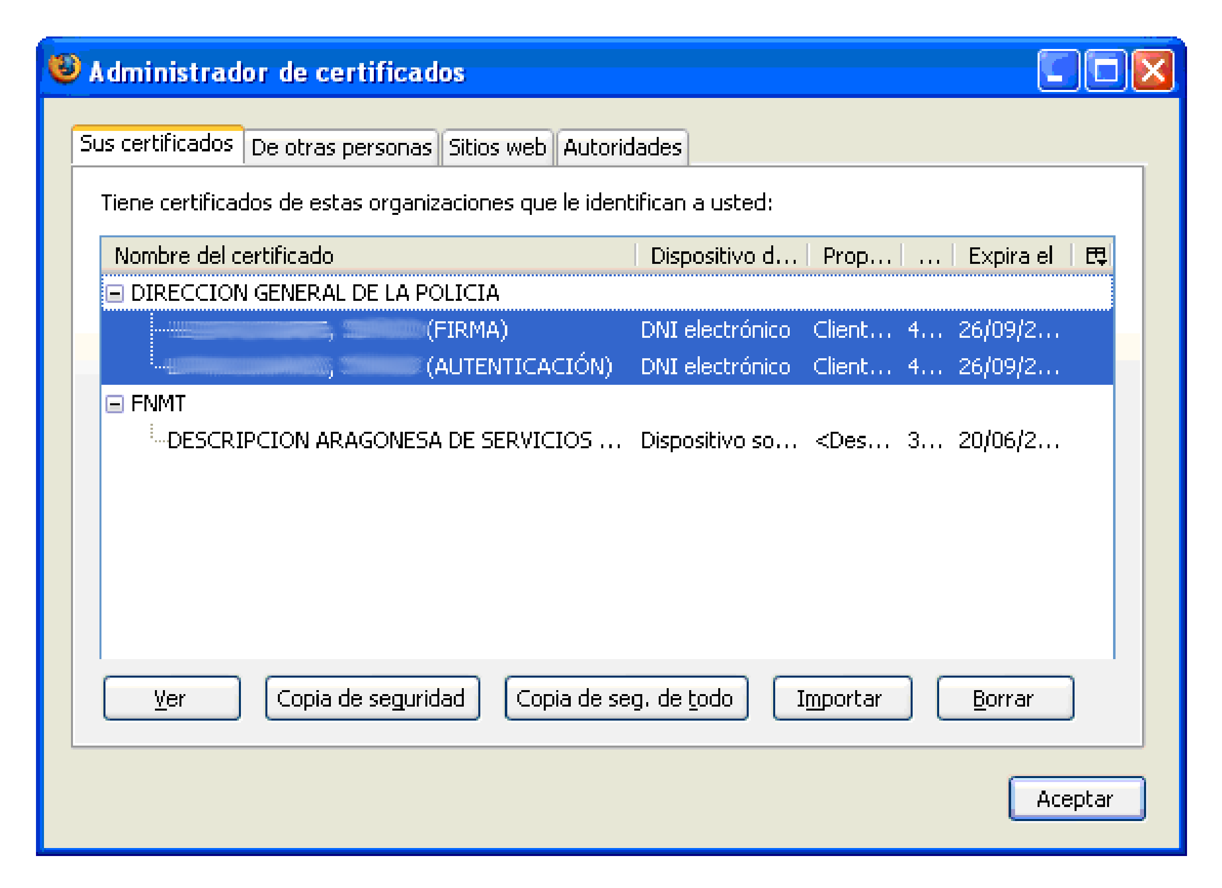
Para comprobar que sus correspondientes drivers han sido instalados correctamente, basta con observar si podemos ver los certificados alojados en las tarjetas desde los distintos almacenes de navegadores.

En Internet Explorer (MS Certificate Store): Herramientas → Opciones de Internet → Pestaña Contenido → Certificados



Certificados del DNI Electrónico en MS Certificate Store

En Mozilla Firefox: Herramientas → Opciones → Avanzado → Pestaña Cifrado → Ver certificados



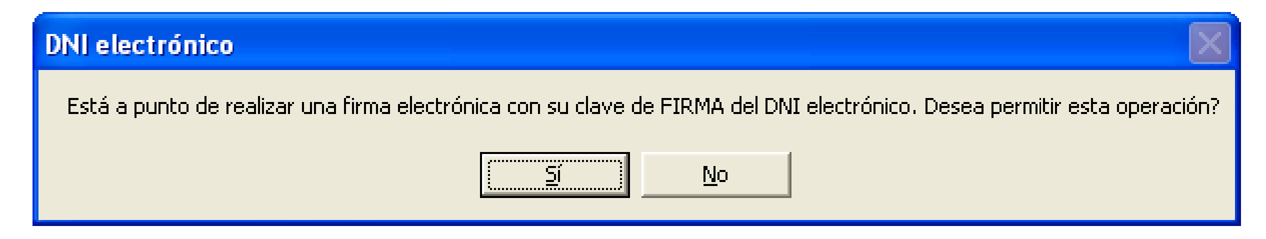
Certificados del DNI Electrónico en Firefox

Estas tarjetas tienen funcionamientos diferentes respecto a su PIN. Mientras que la tarjeta CERES solo pide el PIN cuando se accede a una clave privada y éste se cachea temporalmente, el DNI Electrónico pide el PIN cada vez que tiene que acceder al propio chip criptográfico, ya sea solamente para acceder al certificado público o para usar la clave privada, adicionalmente cuando se vaya a hacer uso de la clave privada de firma, aparecerá un aviso para indicar que esta apunto de realizarse una firma electrónica reconocida (Ley 59/2003).



Petición del PIN del DNI Electrónico

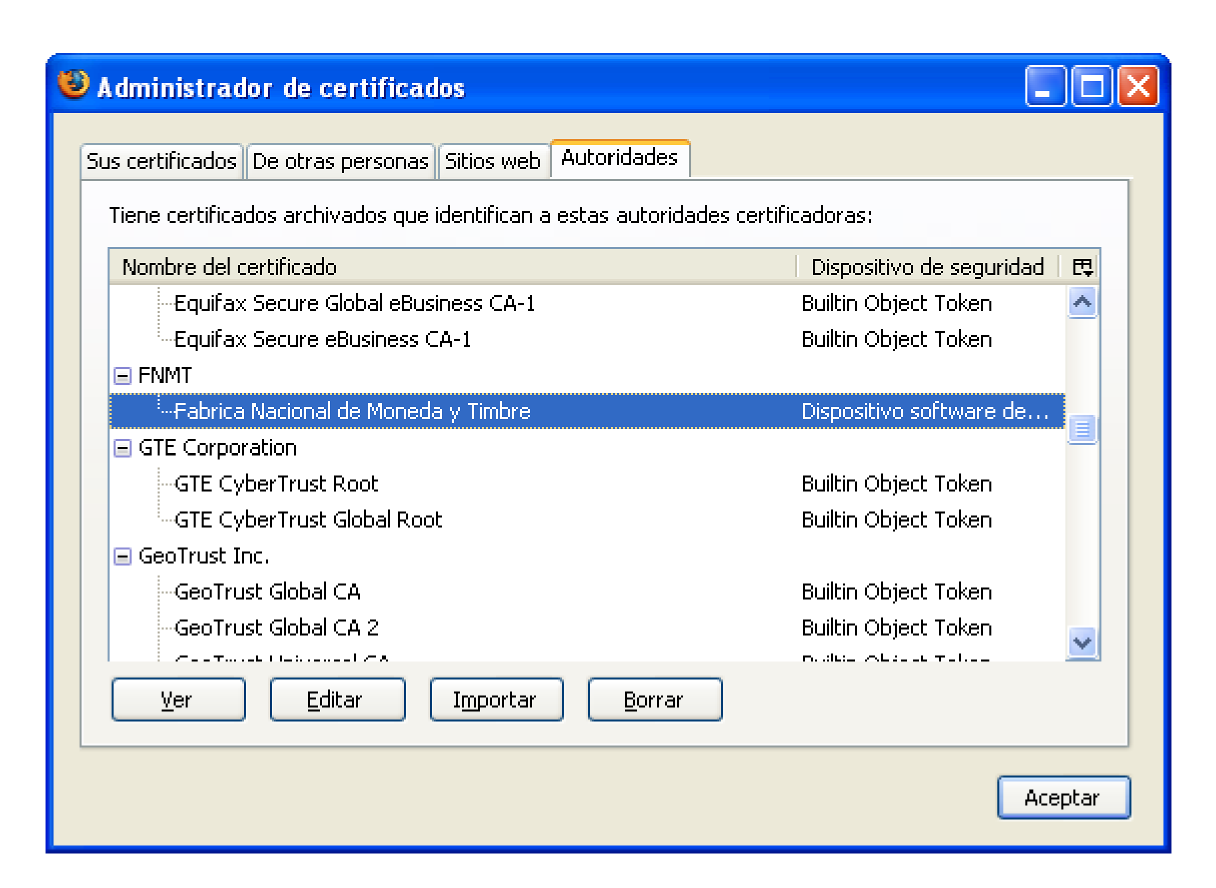




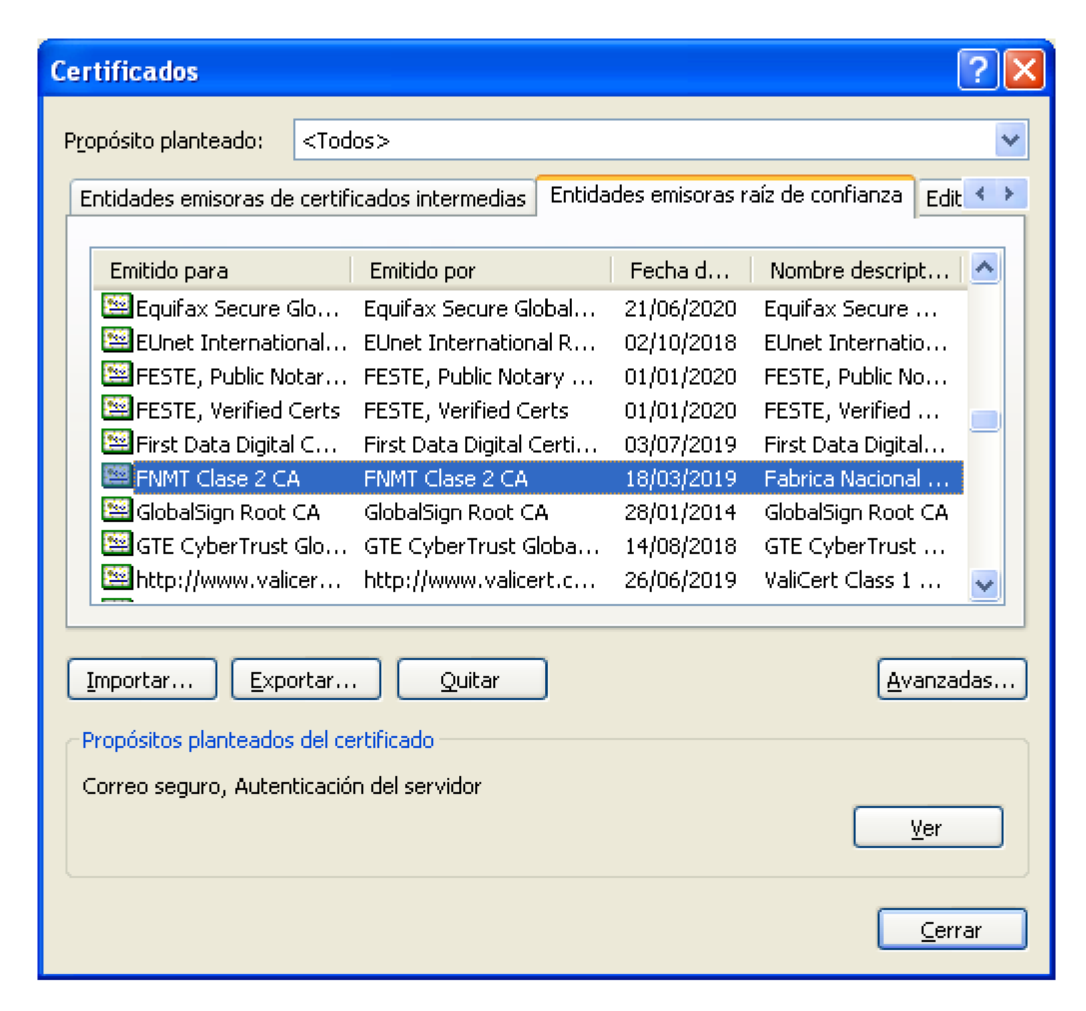
Aviso del DNI Electrónico de creación de firma electrónica reconocida

1.1.3. Certificados Raíz

Los certificados raíz de las Autoridades de Certificación emisoras de los certificados con los que vamos a trabajar, deben estar instalados tanto en el MS Certificate Store como en los almacenes de los diversos clientes que no usen el MS Certificate Store (Firefox, Thunderbird…).

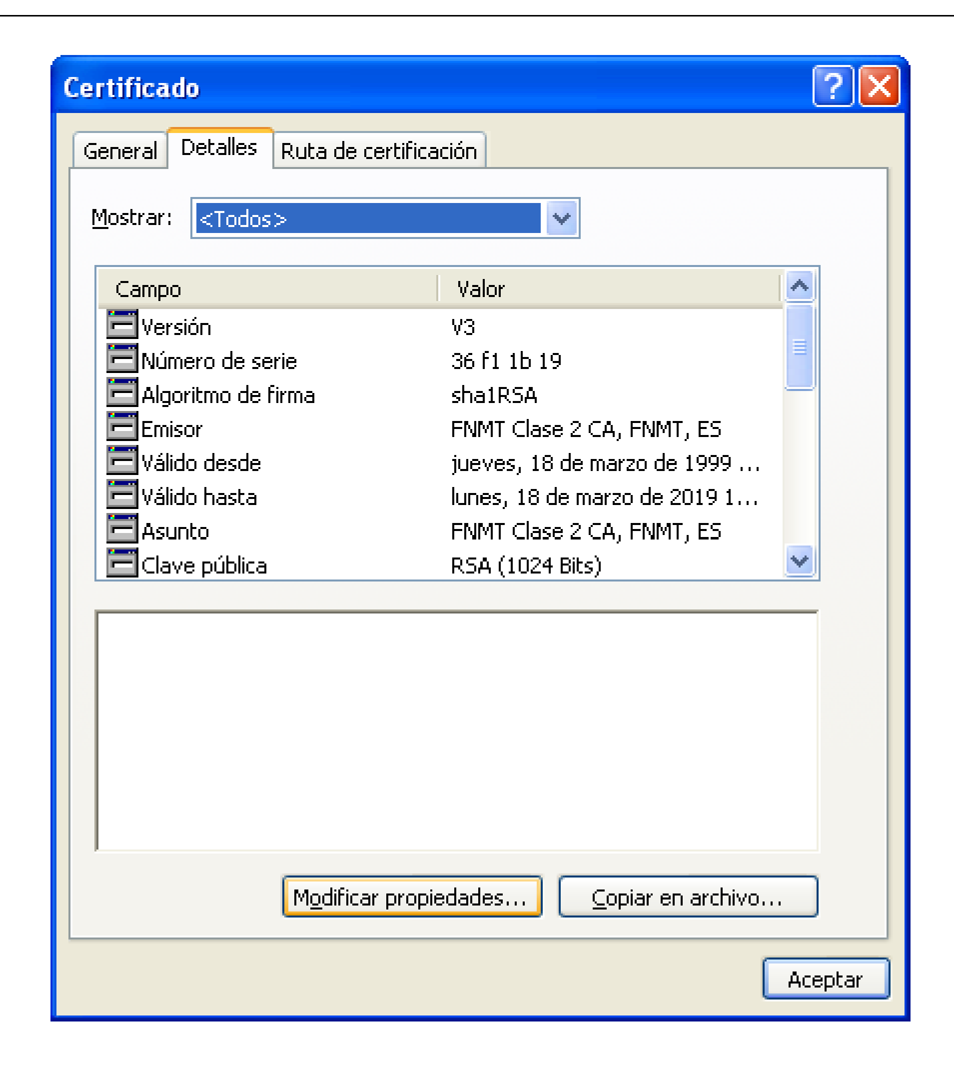


Almacén de certificados de Firefox



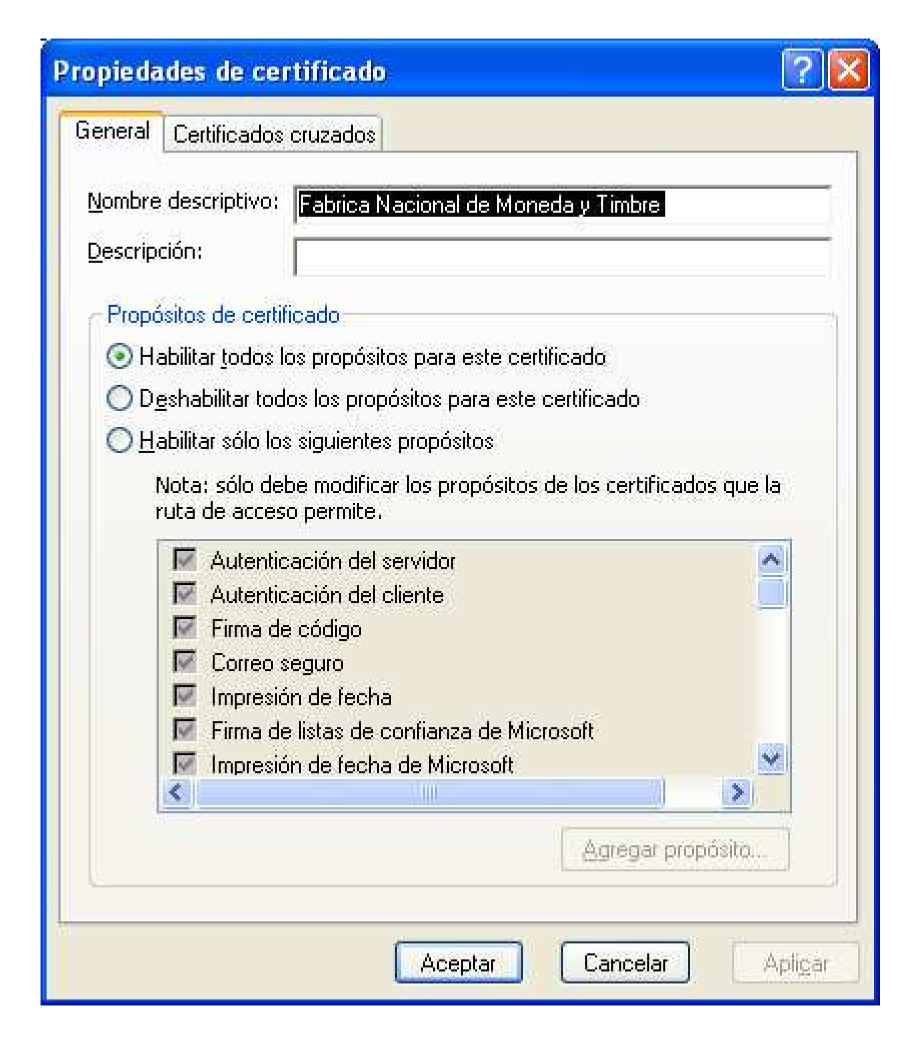
Almacén de certificados MS Certificate Store

En el MS Certificate Store el certificado raíz de la FNMT debe estar habilitado para soportar todos los propósitos. Para ello hacer doble clic en el certificado **FNMT Clase 2** donde aparecerá la siguiente ventana:



En el botón de *Modificar propiedades…* de la pestaña *Detalles* de las propiedades de un certificado, deben habilitarse todos los propósitos para este certificado.





Deben estar habilitados todos los propósitos para este certificado.

1.1.4. Java Runtime Environment (JRE)

Para la utilización del componente cliente, será necesario tener instalada la máquina virtual de Java en sus versiones **JRE 1.6** (desde 1.6.0_1 hasta 1.6.0_45) o **JRE 1.7** (desde 1.7.0_01 hasta 1.7.0_25).Se ha realizado pruebas hasta la versión 1.7.0.51 con la cual se resuelven algunos problemas/bugs con los avisos de seguridad.

1.1.5. Navegador

Con la actual versión del componente cliente se soportan los siguientes navegadores:

- **MS Internet Explorer** 7, 8 y 9 bajo **MS Windows XP/Vista/Windows 7**
- **Mozilla Firefox** (desde 3.6 hasta 22) bajo **MS Windows XP/Vista/Windows 7** y **GNU/Linux** y **Ubuntu 8**

- **Chrome** (desde 11 hasta 28) **MS Windows XP/Vista/Windows 7**
- **Opera** (11.51)

1.1.6. Permisos

Para la correcta instalación del Componente Cliente de Firma, es necesario disponer de permisos de administrador en la primera ejecución.

Una vez realizada la instalación y si ésta ha sido correcta, el usuario no necesita de más privilegios de instalación para ejecutarlo.

Entidad Pública Aragonesa de Servicios Telemáticos
Pº María Agustín 25-27-29 • 50071 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4395
www.aragon.es

2. Proceso Instalación

Cuando se accede al sitio que requiera el uso del componente cliente, si este no está instalado todavía, se procede a su instalación online automática antes de su ejecución.

Para la instalación de del componente cliente se deben cumplir unos requisitos básicos:

- Navegador compatible
- Máquina Virtual Java (JRE) compatible
- El navegador debe tener habilitada la funcionalidad para ejecutar JavaScript
- El navegador debe tener las ventanas Emergentes activadas para el sitio que se esta integrando con el componente cliente.
- Si usa **Windows XP** con cuentas de usuario limitadas, debe ejecutar el navegador con el usuario administrador (únicamente es necesario para el proceso de instalación).
- Si usa **Windows vista** o **Windows 7**, debe ejecutar el navegador con permisos de administrador (únicamente es necesario para el proceso de instalación).

Durante la instalación pueden darse algunos errores. Para ver la solución a posibles errores de instalación ver la sección “Problemas y Soluciones”.

El componente cliente se descarga y se instala automáticamente en la máquina local del usuario, ahorrando así, las constantes descargas de jars en cada ejecución del Applet.

Para ser independiente del Sistema Operativo usado, la instalación se sitúa en la carpeta de la máquina virtual de Java, de manera que los archivos necesarios se alojarán en la carpeta /lib/ext de la JRE. (Ej. C:/Archivos de Programas/Java/JRE_utilizada/lib/ext)

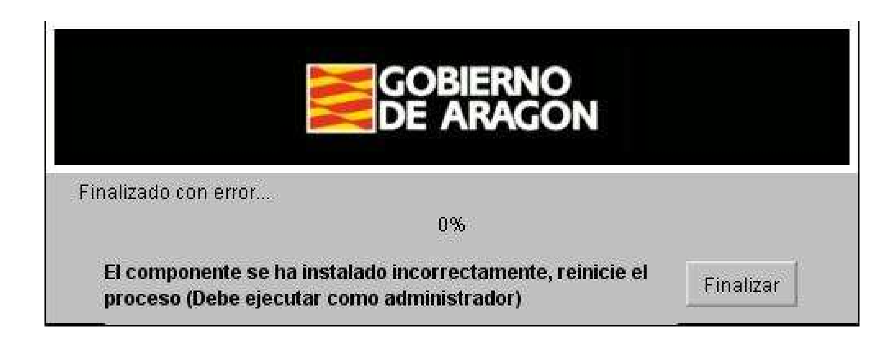
Además, dentro de la carpeta de usuario se creará una carpeta “WebSigner” que alojará las diferentes versiones del componente instalado donde almacenará:

- SystemLibs: Librerías del sistema (DLLs) que se copian a este directorio para tener un control exacto de la carga de las mismas sin depender de posibles versiones obsoletas instaladas en la máquina.

2.1. Instalación Paso a Paso

Para la instalación/actualización de una nueva versión del componente cliente, es necesario acceder vía web y con permisos de administrador a una pagina que lo cargue:

Si ejecuta el navegador sin permisos de administrador, recibirá un aviso de error en la instalación, en este caso debe cerrar el navegador y volver a abrirlo ejecutándolo como administrador:



En caso de tener instaladas versiones anteriores le aparecerá la siguiente pantalla preguntándole si desea actualizar la versión:



Si no dispone de ninguna versión instalada en su entorno, o una vez aceptada la instalación en caso de tener otras versiones del componente instaladas, se lanzaría el proceso de instalación:



Y finalmente si todo ha ido bien, se le pediría reiniciar el navegador:



Una vez realizado este proceso, el usuario podrá ejecutar el navegador de manera normal para usar el componente cliente de firma.

3. Proceso Desinstalación

Para desinstalar WebSigner manualmente será necesario realizar dos acciones para que el proceso de desinstalación sea completo.

3.1. Eliminación del componente

Para la desinstalación manual se deben eliminar los archivos anteriormente citados situados en la carpeta <plug-in JRE path>/lib/ext (únicamente los archivos que tienen referencia al componente **ws63_*)**

dnsns.jar	9 KB	Executable Jar File	25/09/2012 10:15
localedata.jar	816 KB	Executable Jar File	25/09/2012 10:16
meta-index	1 KB	Archivo	25/09/2012 10:15
sunjce_provider.jar	167 KB	Executable Jar File	25/09/2012 10:15
sunmscapi.jar	35 KB	Executable Jar File	25/09/2012 10:15
sunpkcs11.jar	227 KB	Executable Jar File	25/09/2012 10:15
ws63_activation.jar	64 KB	Executable Jar File	25/09/2012 12:56
ws63_ASFXMLSec.jar	398 KB	Executable Jar File	25/09/2012 12:56
ws63_bcprov-jdk14-139.jar	2.262 KB	Executable Jar File	25/09/2012 12:56
ws63_BinaryCipher.jar	22 KB	Executable Jar File	25/09/2012 12:56
ws63_BinarySign.jar	62 KB	Executable Jar File	25/09/2012 12:56
ws63_CAPIProv.jar	156 KB	Executable Jar File	25/09/2012 12:56
ws63_commons-beanutils-1.8...	227 KB	Executable Jar File	25/09/2012 12:56
ws63_commons-codec-1.3.jar	51 KB	Executable Jar File	25/09/2012 12:56
ws63_commons-collections-3....	614 KB	Executable Jar File	25/09/2012 12:56
ws63_commons-httpclient-3.1...	314 KB	Executable Jar File	25/09/2012 12:56
ws63_commons-jxpath-1.3.jar	301 KB	Executable Jar File	25/09/2012 12:56
ws63_commons-logging-1.0.4...	36 KB	Executable Jar File	25/09/2012 12:56
ws63_Core.jar	75 KB	Executable Jar File	25/09/2012 12:56
ws63_Easycert.jar	55 KB	Executable Jar File	25/09/2012 12:56
ws63_Graphic.jar	35 KB	Executable Jar File	25/09/2012 12:56
ws63_jaxb.jar	2.204 KB	Executable Jar File	25/09/2012 12:56
ws63_Launcher.jar	23 KB	Executable Jar File	25/09/2012 12:56
ws63_mail.jar	470 KB	Executable Jar File	25/09/2012 12:56
ws63_NoGraphic.jar	11 KB	Executable Jar File	25/09/2012 12:56
ws63_PDFSign.jar	2.182 KB	Executable Jar File	25/09/2012 12:56
ws63_tbs_certificate_info_ex...	35 KB	Executable Jar File	25/09/2012 12:56
ws63_tbs_util.jar	59 KB	Executable Jar File	25/09/2012 12:56
ws63_tbsconnection.jar	102 KB	Executable Jar File	25/09/2012 12:56
ws63_tbscrypto.jar	829 KB	Executable Jar File	25/09/2012 12:56
ws63_Theme.jar	27 KB	Executable Jar File	25/09/2012 12:56
ws63_Util.jar	649 KB	Executable Jar File	25/09/2012 12:56
ws63_xalan2.6.0.jar	3.358 KB	Executable Jar File	25/09/2012 12:56
ws63_xerces2.7.1.jar	1.767 KB	Executable Jar File	25/09/2012 12:56
ws63_XMLCipher.jar	71 KB	Executable Jar File	25/09/2012 12:56
ws63_xmlcomponent.jar	835 KB	Executable Jar File	25/09/2012 12:56
ws63_XMLSign.jar	45 KB	Executable Jar File	25/09/2012 12:56

Entidad Pública Aragonesa de Servicios Telemáticos
Pº María Agustín 25-27-29 • 50071 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4395
www.aragon.es

3.2. Borrado de la cache de JAVA

En caso de tener la cache de Java activada, será necesario borrar los datos correspondientes para evitar así que se ocasionen problemas en futuras ejecuciones

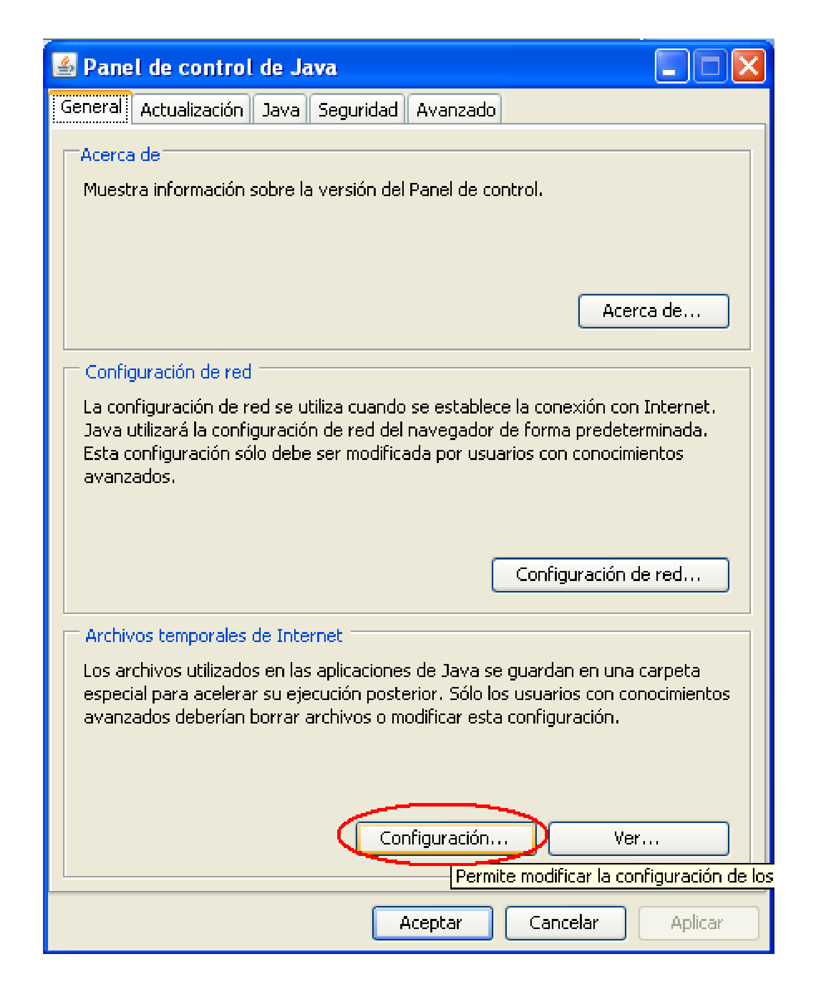
La forma de desinstalar el componente cliente es borrando la cache de Java desde el panel de control de Java, dicho panel puede aparecer en el panel de control del sistema operativo con el nombre de 'Java'. En Windows XP se encontraría en "Inicio->Panel de Control->Java"

Si en el Panel de Control no aparece el panel de control de Java (depende de cómo se haya realizado la instalación), se puede arrancar directamente de su ejecutable alojado en: DirectorioJRE\bin\javacpl.exe

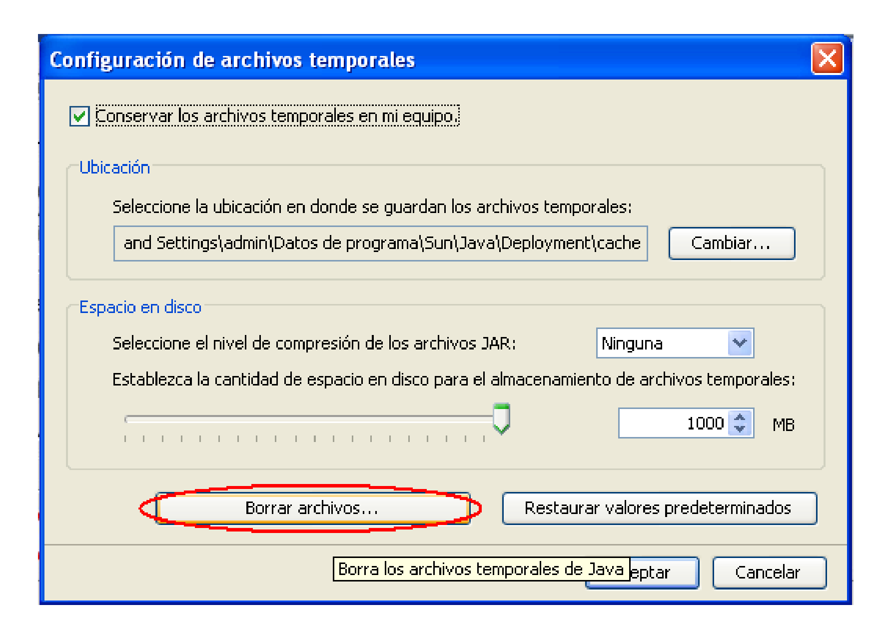
El panel de control de Java cambia según la versión de la JRE.

Ir a la pestaña "General" y pulsar sobre el botón "Configuración…":





Pulsar sobre el botón “Borrar archivos…”:



Marcar la check “Aplicaciones y applets” y pulsar sobre el botón “Aceptar”. Si la check “Aplicaciones y applets” aparece deshabilitada es porque la check “Conservar los archivos

temporales en mi equipo." que se puede ver en la captura del paso 2 esta sin marcar por lo que no hay nada que borrar.



4. Problemas y Soluciones

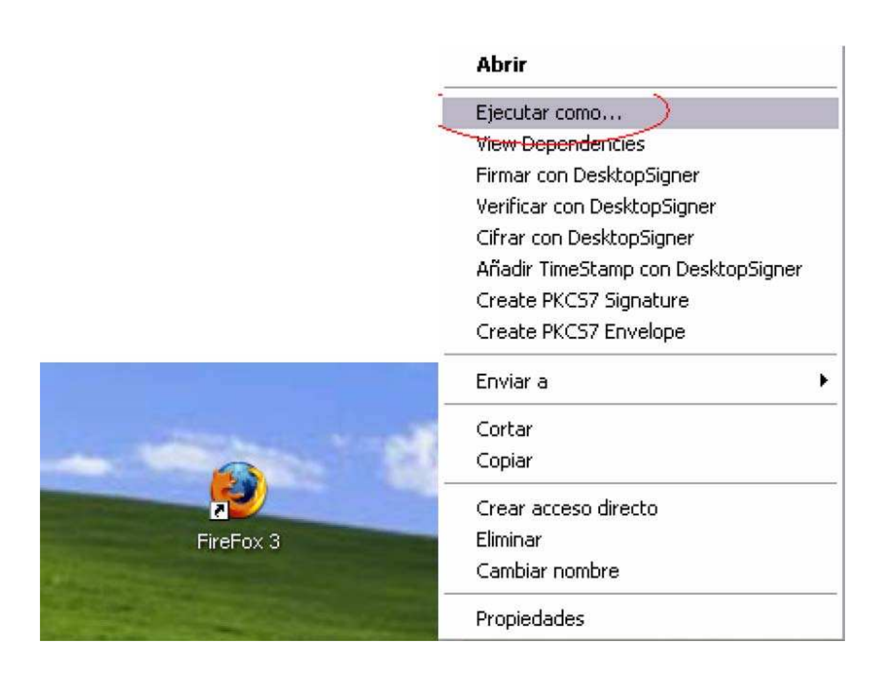
4.1. Instalación incorrecta por requerir permisos de Administrador

Debido a limitaciones de seguridad de las versiones más recientes de la Máquina Virtual Java es necesario disponer de permisos de administrador para poder instalar el Componente de Firma (en la primera ejecución). Una vez instalado el Componente de Firma, en posteriores ejecuciones, se puede iniciar el navegador con los permisos habituales.

Aunque el usuario posea permisos de administrador, en algunos Sistemas Operativos (Windows Vista/7) el navegador se lanza por defecto sin permisos de administrador, por lo que será necesario la primera vez lanzar el navegador con permisos de administrador de forma explícita.

Dependiendo del sistema operativo la inicialización del navegador en modo administrador se realizará de una forma diferente:

- En Windows, pulsando con el botón derecho sobre el icono de navegador hay que seleccionar la opción "Ejecutar como" y en la ventana elegir la opción "El siguiente usuario" y elegir la usuario "Administrador" y finalmente "Aceptar"
- En Linux, será necesario iniciar una sesión como administrador (comando "su -") y desde esa sesión iniciar el navegador.



Una vez realizada la instalación y si ésta ha sido correcta, el usuario no necesita de más privilegios de instalación para ejecutarlo.

4.2. Ventanas emergentes desactivadas

En algunos casos es posible que el componente necesite tener las ventanas Emergentes activadas para el sitio que se esta integrando con el componente cliente.

No aparece nada en la pantalla. Según versiones del navegador avisa de que se esta intentando mostrar una pantalla y en otras muestra un icono en la barra de estado.

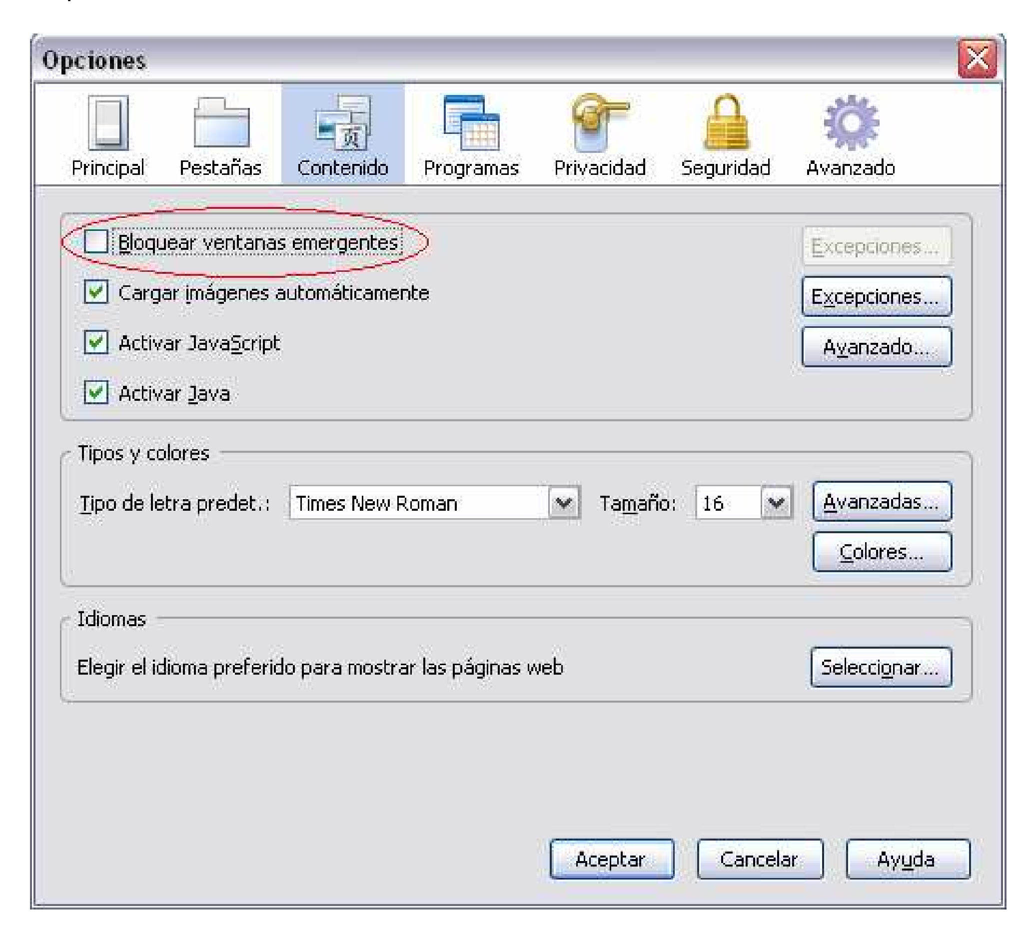
Se debe permitir mostrar pantallas emergentes al sitio.

Cunando no muestra la petición de ventanas emergentes no se carga la maquina virtual.

Mozilla Firefox 3

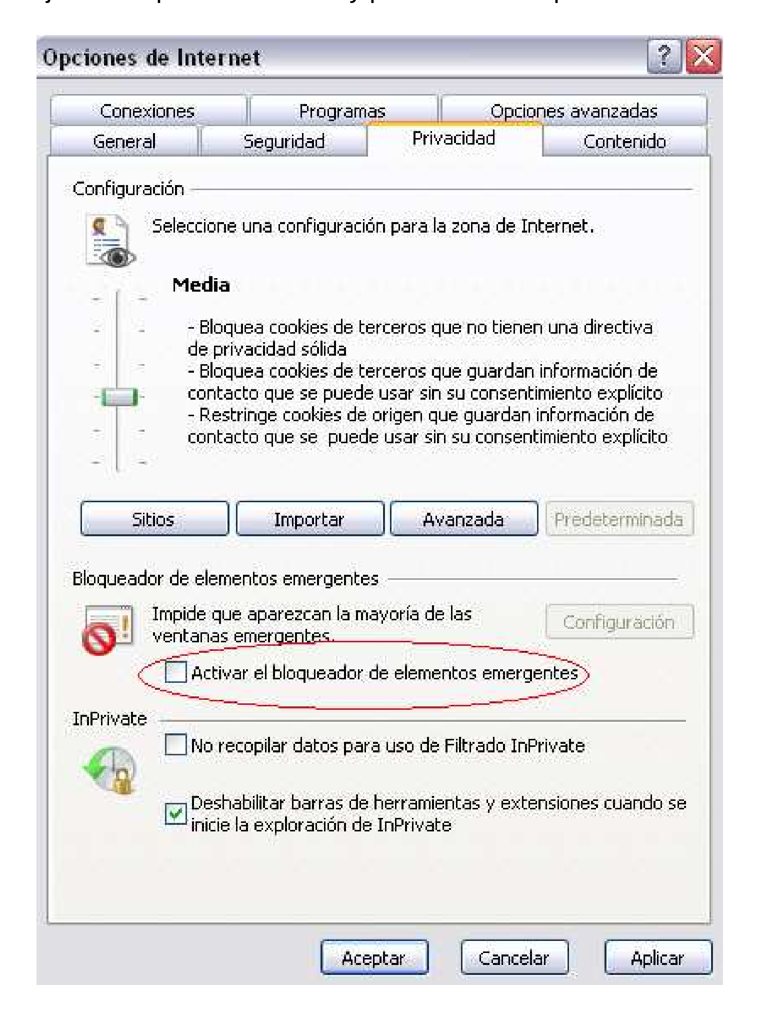
En este caso habrá que desactivar la opción “Bloquear ventanas emergentes”,

o bien añadir una excepción al sitio desde el cual se accede al componente cliente en el botón “Excepciones…” situado a la derecha de “Bloquear ventanas emergentes”. En Herramientas->Opciones->Contenido



MS Internet Explorer

En las últimas versiones de IExplorer podemos desactivar la opción de "Activar el bloqueador de elementos emergentes" en Herramientas->Opciones de Internet->Privacidad. También podemos dejar esta opción habilitada y poner una excepción en el menú de "Configuración".

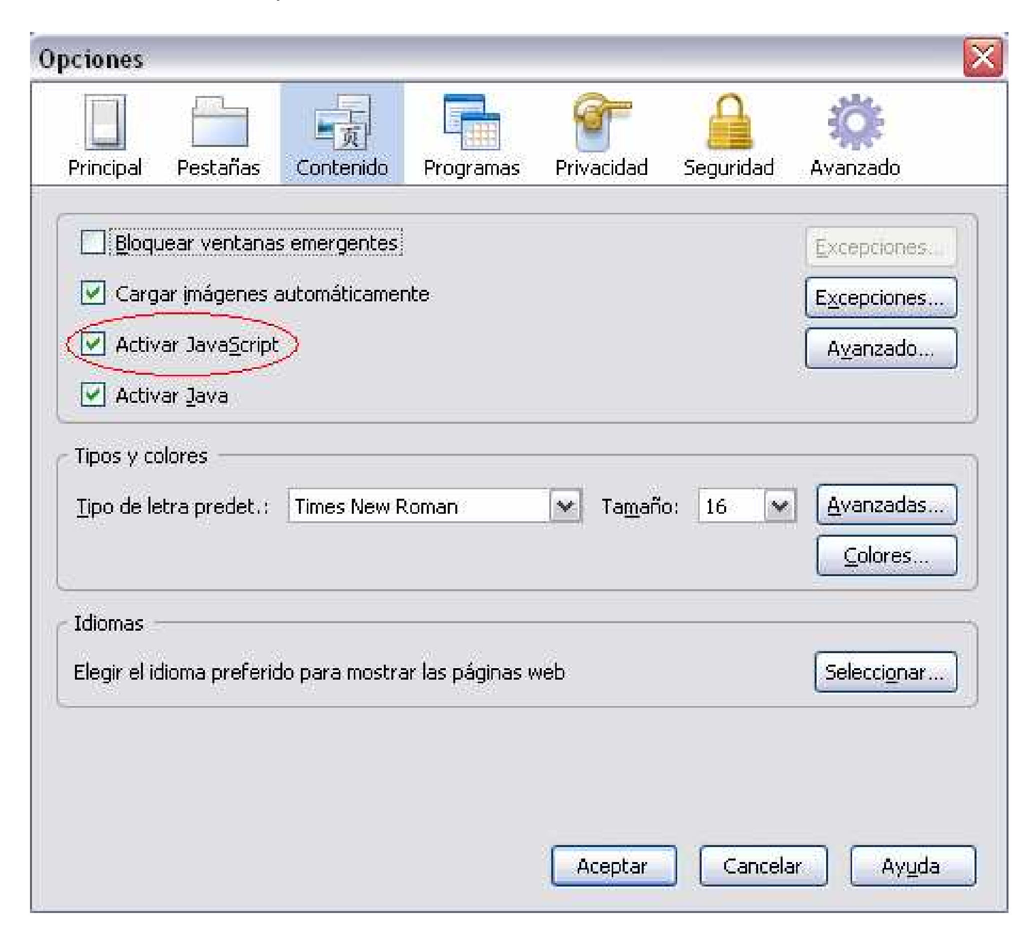


4.3. No hay permisos de ejecución de JavaScript

Hay que permitir ejecutar JavaScript para que funcione correctamente.

Mozilla Firefox 3

En Herramientas->Opciones->Contenido



Mozilla Firefox no mostrara ningún mensaje avisando de este hecho.

4.4. Una vez aceptado todo no sucede nada

Hay que recargar como mínimo las paginas Web para que lance de nuevo la ejecución del plug-in Java.

Según versión del navegador también puede ser necesario reiniciar todo el navegador.

En Sistemas Operativos de 64 bits “Windows 64 bits” (Vista/7) debe tener en cuenta que para el correcto funcionamiento del componente es necesario instalar un entorno de ejecución de Java en 32 bits, y no una variante de 64 bits (tanto del navegador como de la máquina virtual de Java).

4.5. No esta instalada la Maquina Virtual Java

Se requiere tener instalada la Máquina Virtual Java en alguna de las versiones compatibles indicadas en este documento.

Se dispone de dos procesos:

- Instalación de cero:

En caso de no disponer de ninguna versión de plugin instalada deberá descargase la JRE (http://www.java.com/es/). Una vez descargada simplemente se debe ejecutar el archivo descargado.

- Actualización:

En caso de disponer de una versión de java actualmente instalada se puede realizar el proceso anterior o en su lugar llevar a cabo una actualización, para ello se deben seguir los siguientes pasos:

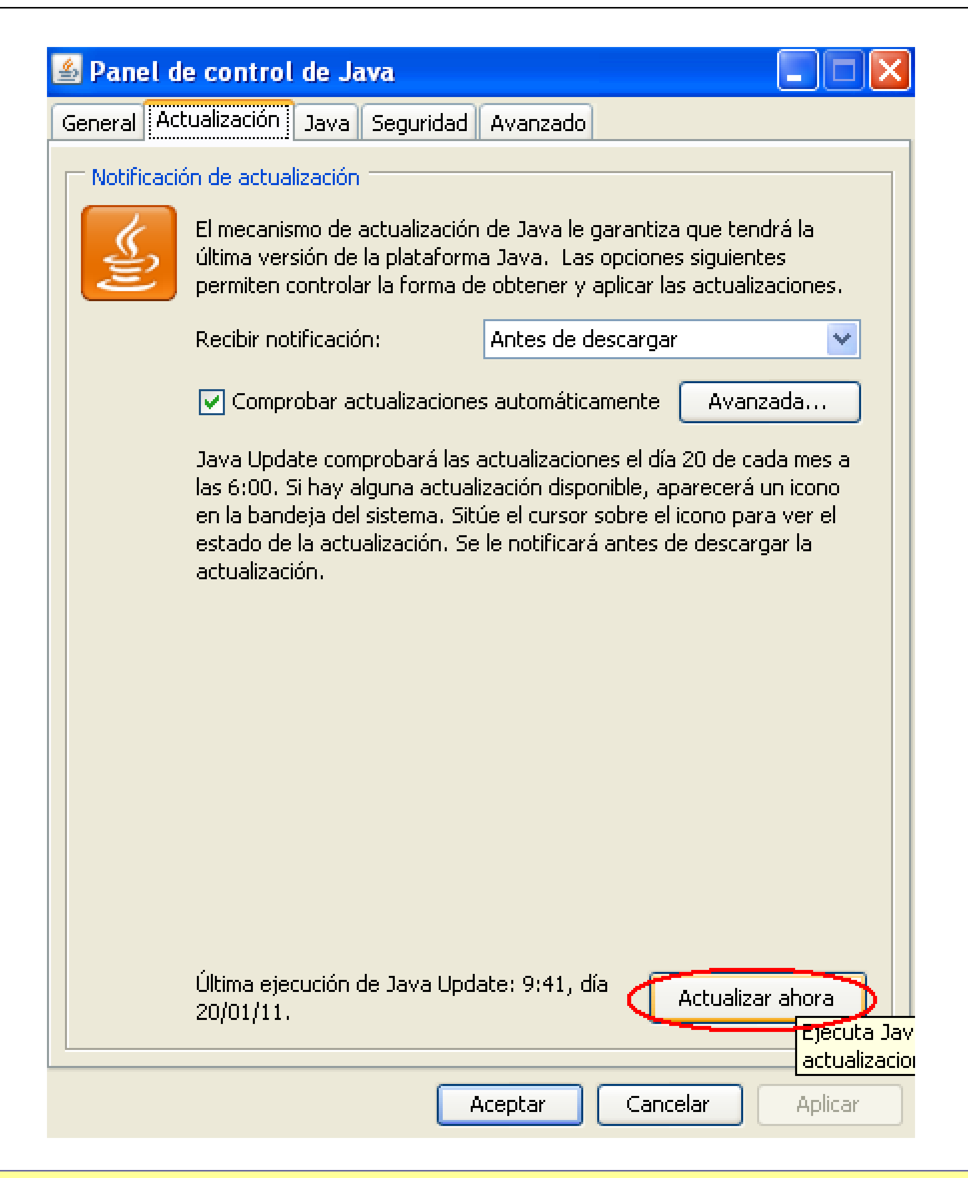
1. Se accede al panel de java disponible en el panel de control de Windows.



2. Accedemos a la pestaña Actualización y pulsamos la opción Actualizar ahora.

Entidad Pública Aragonesa de Servicios Telemáticos
Pº María Agustín 25-27-29 • 50071 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4395
www.aragon.es





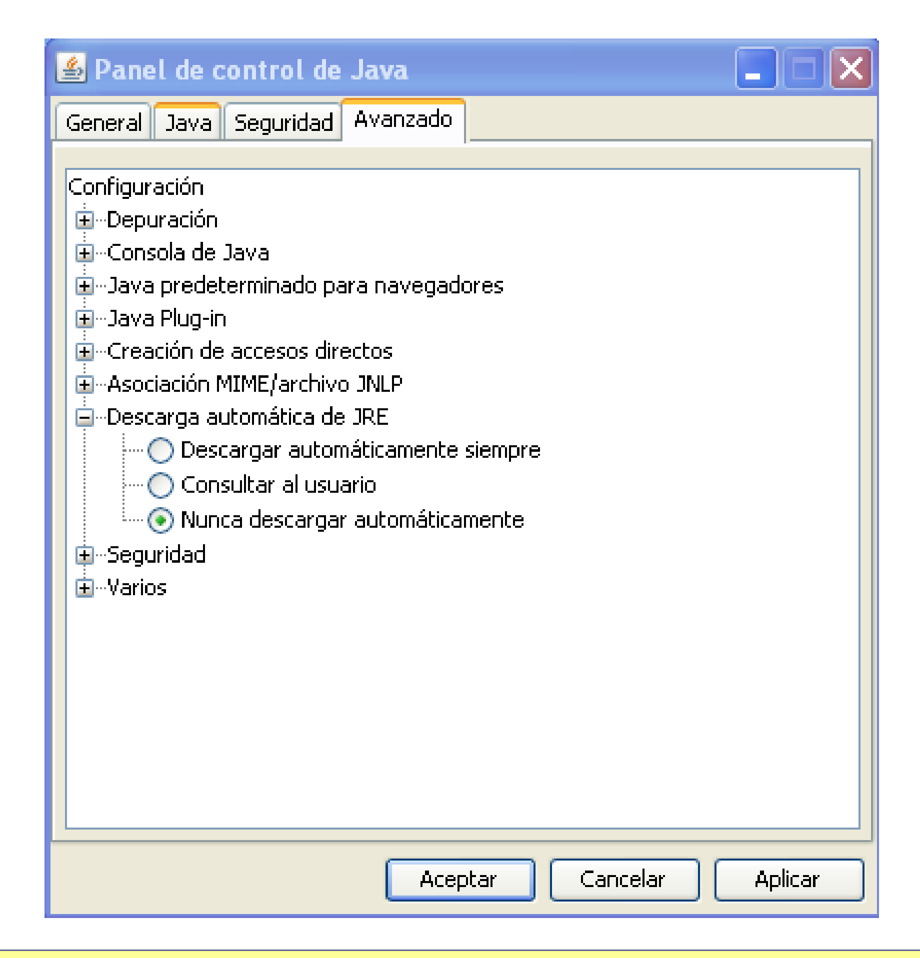
NOTA: Esta ventana puede cambiar según las diferentes versiones de JRE instaladas.

4.6. Problema al actualizar la Maquina Virtual Java

Cuando se actualiza la JRE en el equipo del usuario, el componente cliente deja de funcionar ya que este se instala dentro de la propia JRE, por lo que se hace necesario volver a instalarlo.

En entornos en los que los usuarios trabajen con cuentas limitadas, recomendamos que en la instalación de la JRE se desmarque la opción de actualización para evitar estos problemas.





NOTA: Esta ventana puede cambiar según las diferentes versiones de JRE instaladas.

4.7. Se produce un error en la carga de certificados

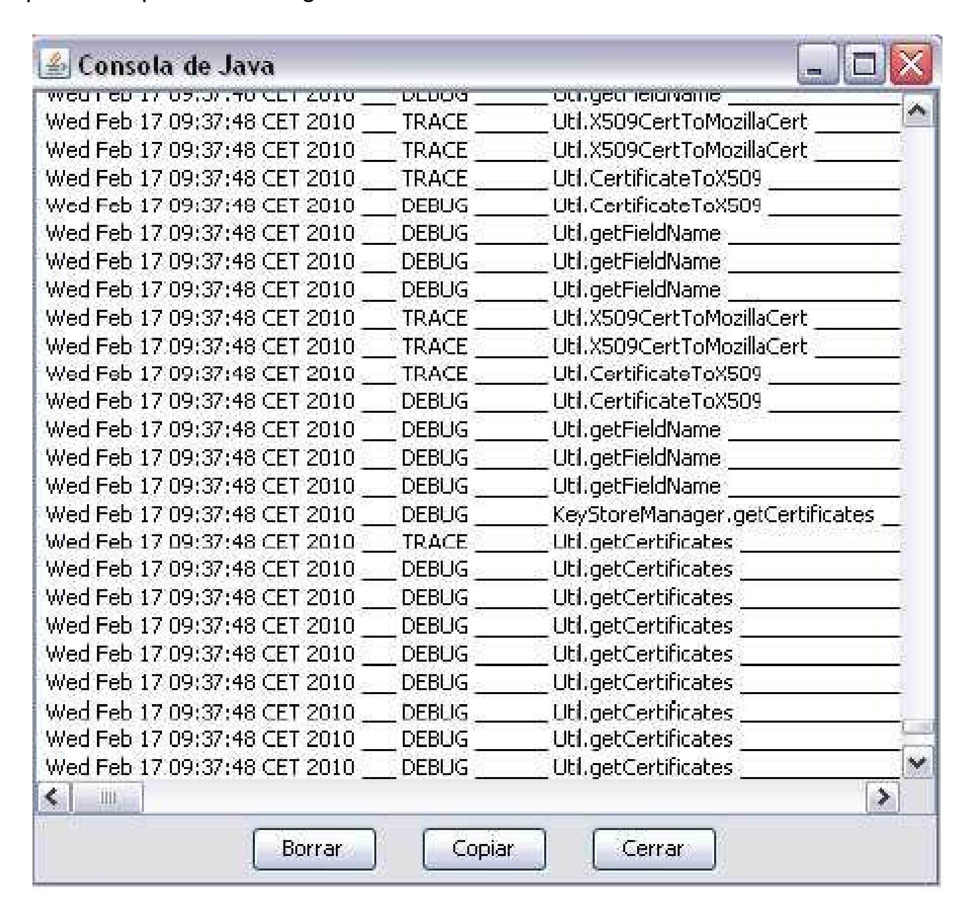
En el momento de la instalación y ejecución del componente puede ocurrir algún error, por lo que si se detecta que el componente no se carga o no se está ejecutando correctamente se debe mirar lo primero de todo, la consola de Java.

Si el navegador correspondiente no ha abierto ésta podemos abrirla nosotros pulsando botón derecho sobre el icono de Java que se encuentra abajo a la derecha de la pantalla y seleccionando en el menú desplegado la opción Abrir Consola:



Entidad Pública Aragonesa de Servicios Telemáticos
Pº María Agustín 25-27-29 • 50071 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4395
www.aragon.es

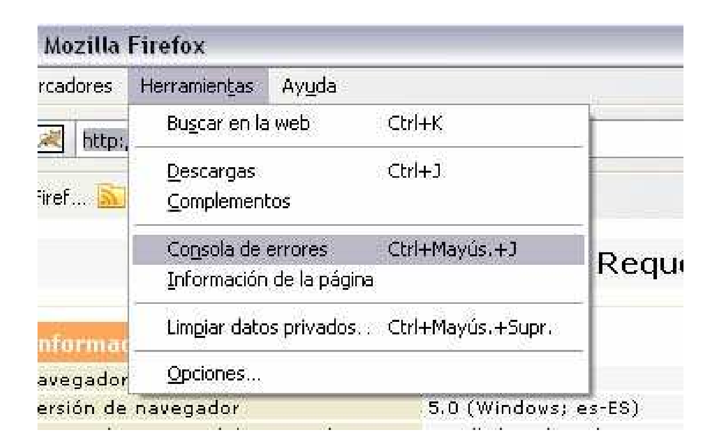
Una vez pulsada aparecerá la siguiente ventana:



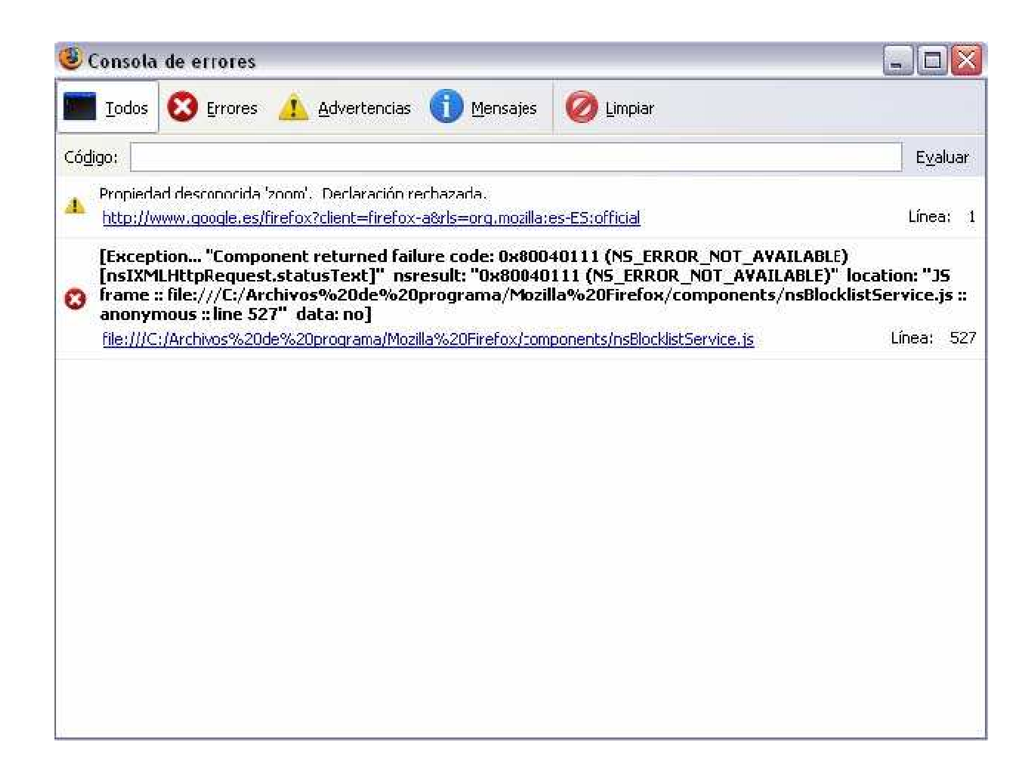
Si ocurriera un error del componente se podría detectar en esta consola de manera rápida, para posteriormente consultar los errores con sus posibles soluciones.

También será de utilidad mirar la consola JavaScript para ver si el error está en los scripts. Esta consola se puede ver en:

Firefox 3

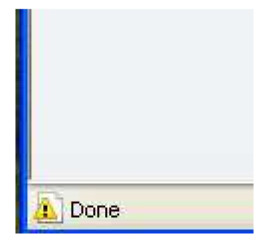


Aparecerá por pantalla una consola con aspecto parecido al siguiente:



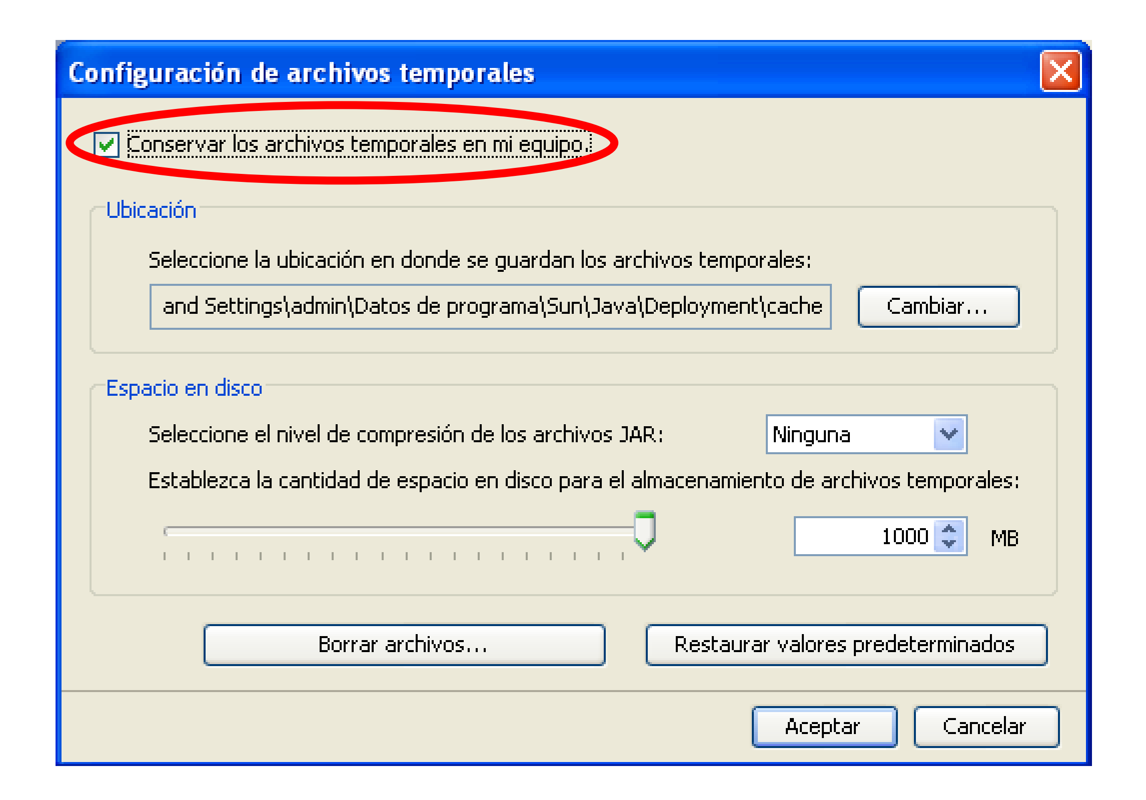
Internet Explorer 7, 8 y 9

Si ocurre un error JavaScript saldrá un icono en la parte inferior izquierda de la ventana del explorador. Si hacemos doble click en este icono se abrirá una ventana con la explicación del error.

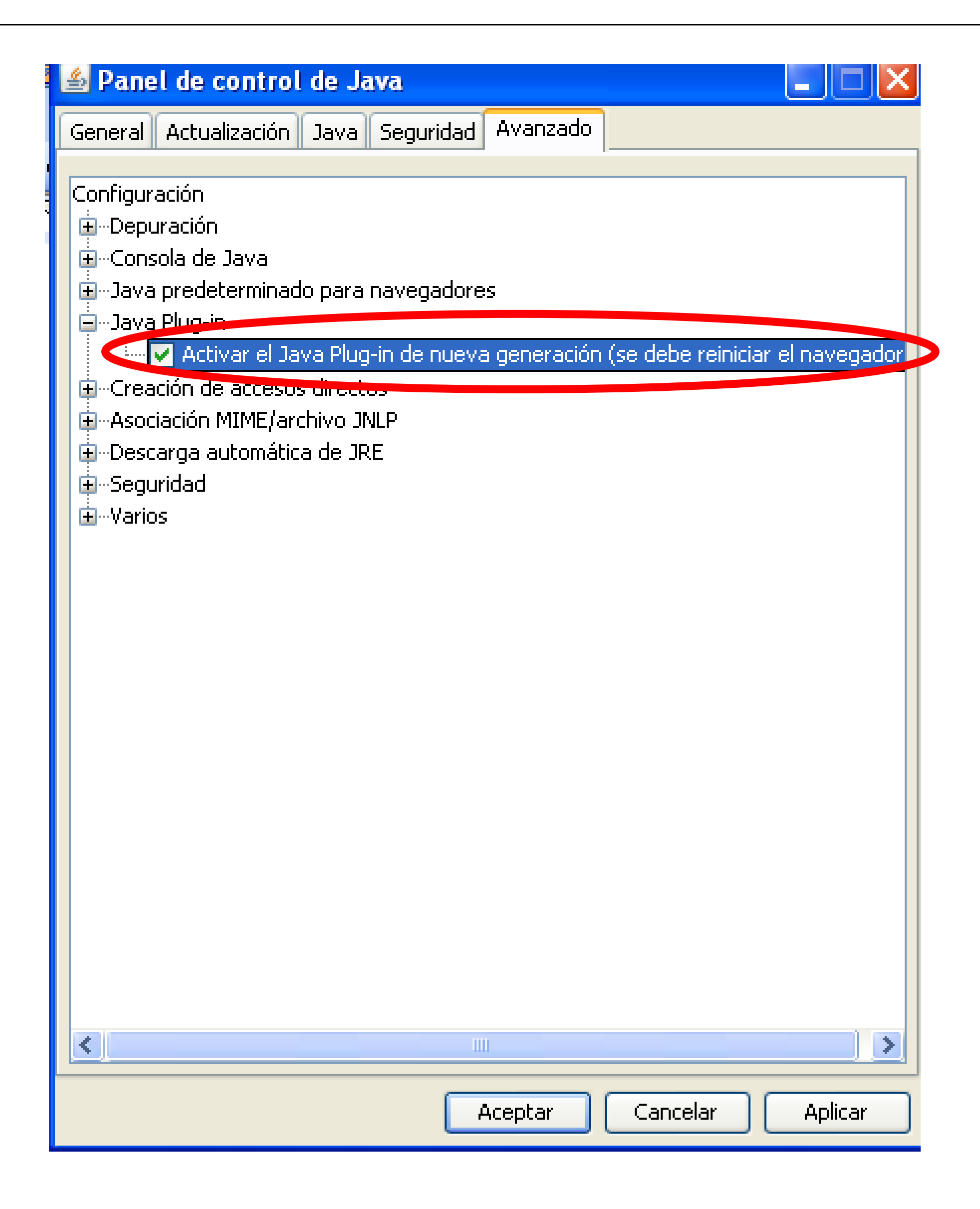


En estos casos, es posible que la versión del panel de control java o la configuración local del panel de control de Java no sea la correcta para el funcionamiento del componente. Para ello, actualice la versión de Java según las indicaciones del punto 4.4.1 y posteriormente compruebe que posee la siguiente configuración:

1. Conservar los archivos temporales en el equipo: Accediendo a la ventana de la consola según las indicaciones del apartado 3, es necesario tener marcada esa propiedad.



2. Si continúan los errores en la ejecución, para navegadores Firefox de versión 3.6.X se han detectado errores en algunas casuísticas en función de la configuración del panel de control de Java. En estos casos es recomendable activar la opción “Java Plug-In” (dicha opción aparece en versiones recientes de la consola de java, por lo que si no aparece es necesario actualizar la consola siguiendo las indicaciones del apartado 4.4) en la misma pestaña ***Avanzado*** indicada en la opción anterior como se indica en la figura:



Entidad Pública Aragonesa de Servicios Telemáticos
Pº María Agustín 25-27-29 • 50071 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4395
www.aragon.es

4.8. Se produce un error al firmar un fichero alojado en el equipo del usuario

Internet Explorer 8 y 9



El problema se debe a una restricción de seguridad que tiene el navegador IExplorer en versiones posteriores a la 7 (el navegador ofusca la ruta del fichero a firmar por lo que el componente cliente de firma no tiene acceso al documento que tiene que firmar, motivo por el cual se produce el error).

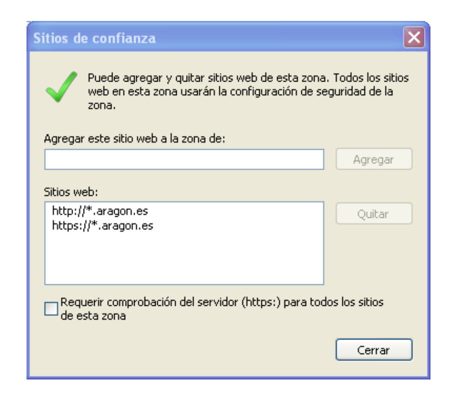
Solución

Dado que es un tema de seguridad y el IExplorer no ofusca la ruta local de los sitios de confianza, una solución al problema seria la siguiente:

Abrir desde el menú de “Herramientas –> Opciones de Internet”, ir a la pestaña de “Seguridad”:



Clickear en el icono de “Sitios de confianza” y posteriormente al botón “sitios”:



Y en la ventana agregar las rutas en los sitios de confianza del usuario http://*.aragon.es y https://*.aragon.es .

4.9. Versiones de Java y Avisos de seguridad

A partir de la versión 1.7.0.21 de java se han realizado cambios que obligan a los applets utilizados a estar firmados, esto hace que con determinadas configuraciones de la JVM el componente cliente sea bloqueado, para ello hemos realizado varias pruebas con las diferentes versiones de java y sus configuraciones que vamos a resumir ahora para resolver posibles problemas.

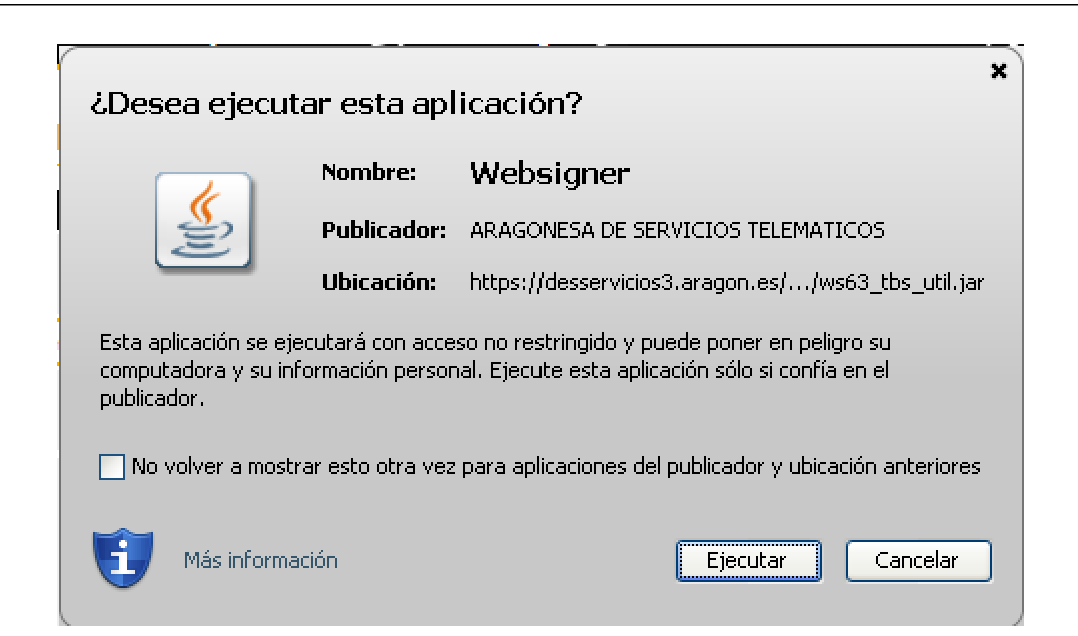
4.9.1. Java 1.7.0.21

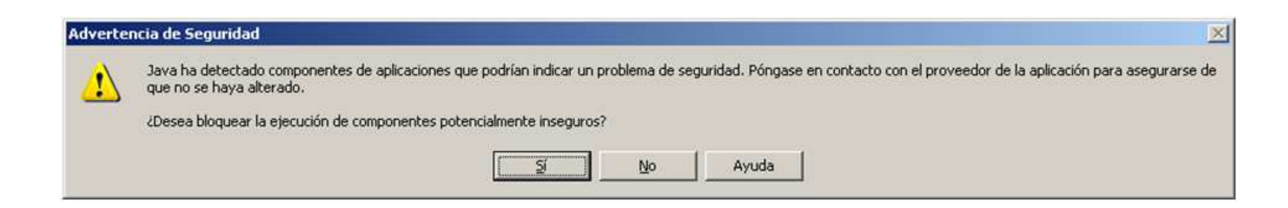
4.9.1.1. Seguridad Alta

Las pruebas para dicha versión se han realizado con la siguiente configuración de seguridad de Java:



Entidad Pública Aragonesa de Servicios Telemáticos
Pº María Agustín 25-27-29 • 50071 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4395
www.aragon.es





Habría que indicar [No], para que la seguridad, no bloquee la instalación de WebSigner.

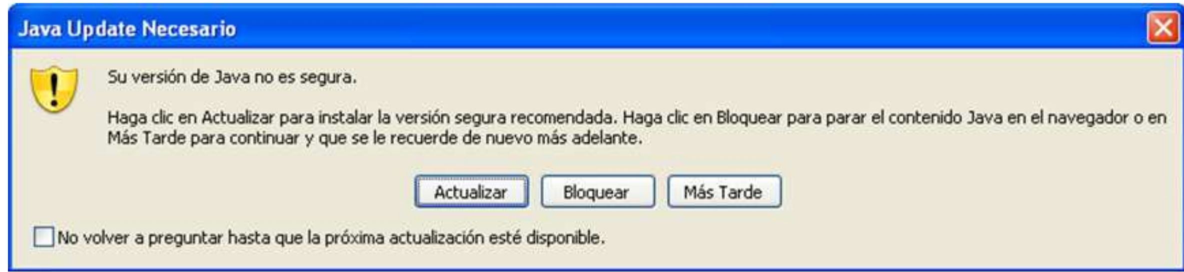
Entidad Pública Aragonesa de Servicios Telemáticos
Pº María Agustín 25-27-29 • 50071 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4395
www.aragon.es

4.9.1.2. Seguridad Media

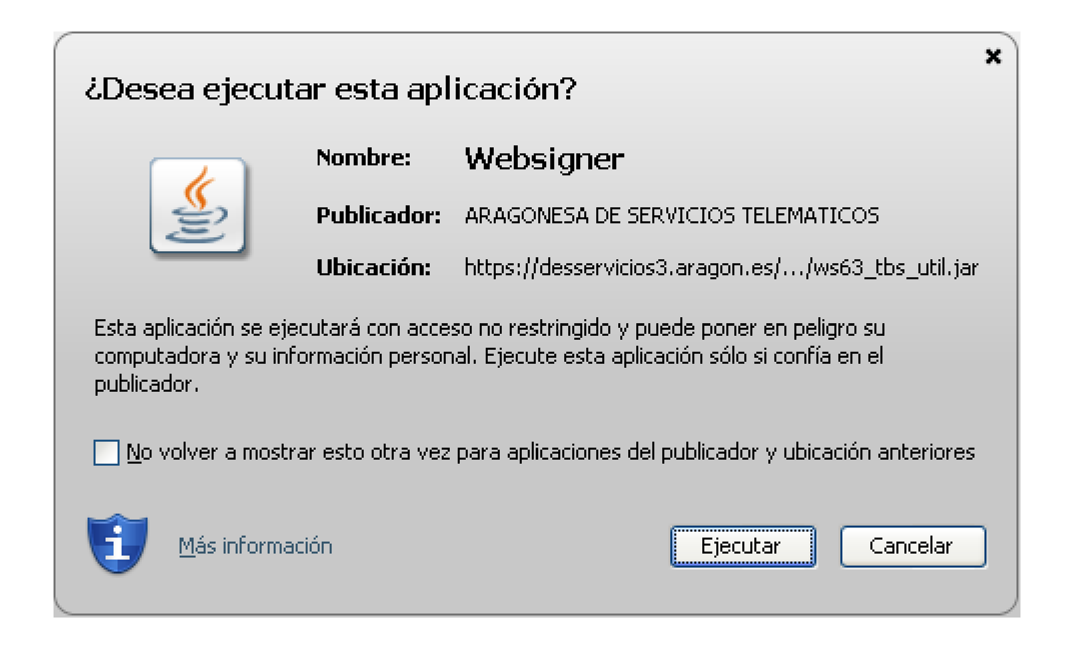
Las pruebas para dicha versión se han realizado con la siguiente configuración de seguridad de Java:



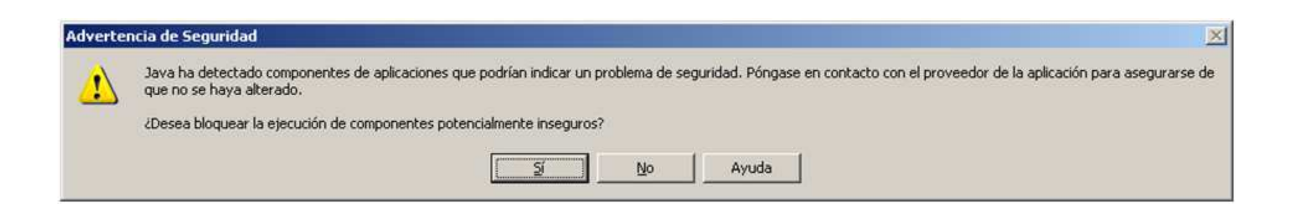
,



Se indica Más Tarde para continuar con la instalación con esta configuración.



Al [Ejecutar], se muestra un nuevo mensaje.



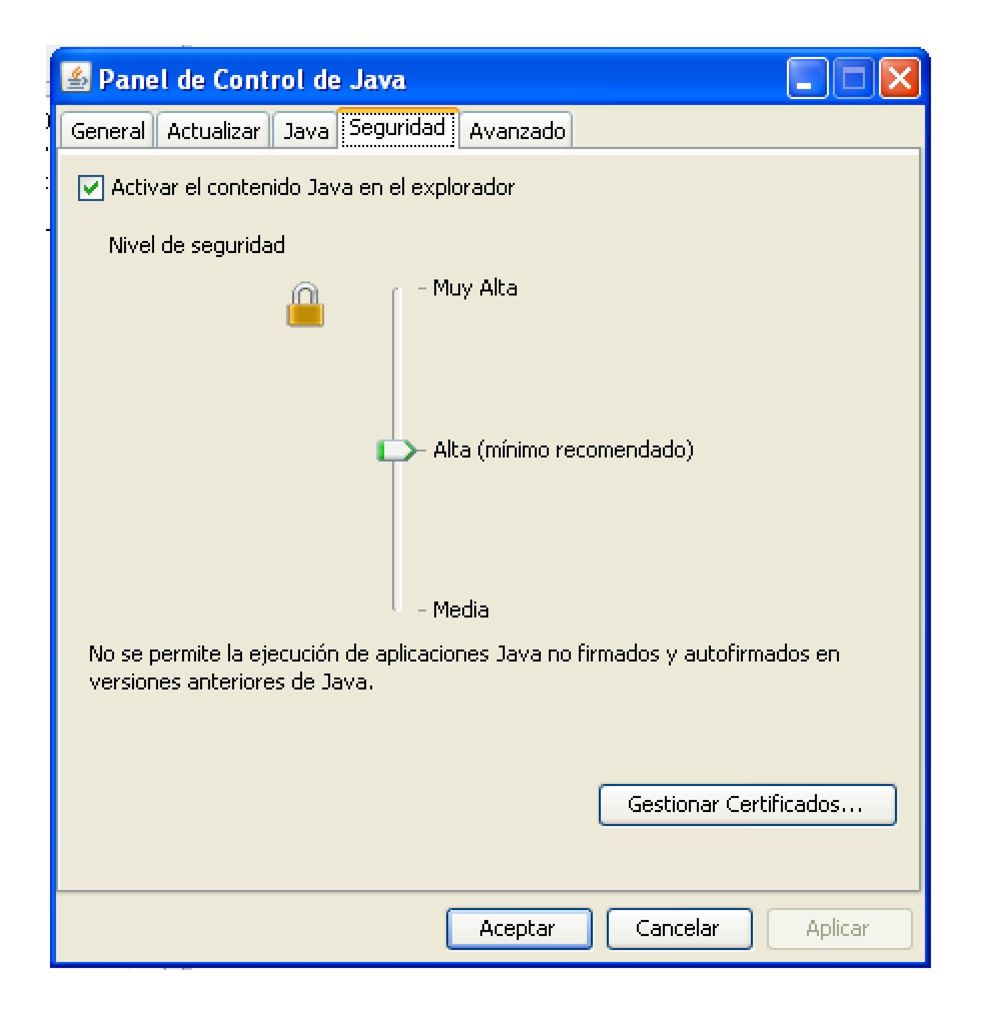
Habría que indicar [No], para que la seguridad, no bloquee la instalación de WebSigner.

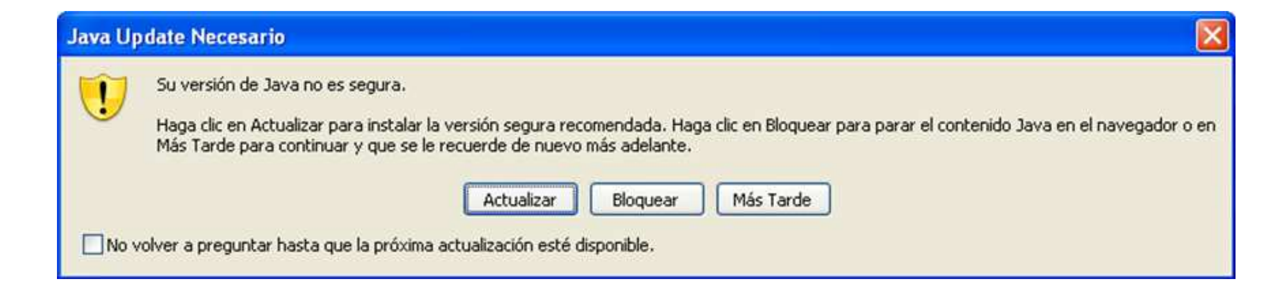
4.9.2. Java 1.7.0.25

El comportamiento de la versión de Java v1.7.0_25 es similar a la v1.7.0_21. La instalación de WebSigner depende del nivel de seguridad de Java

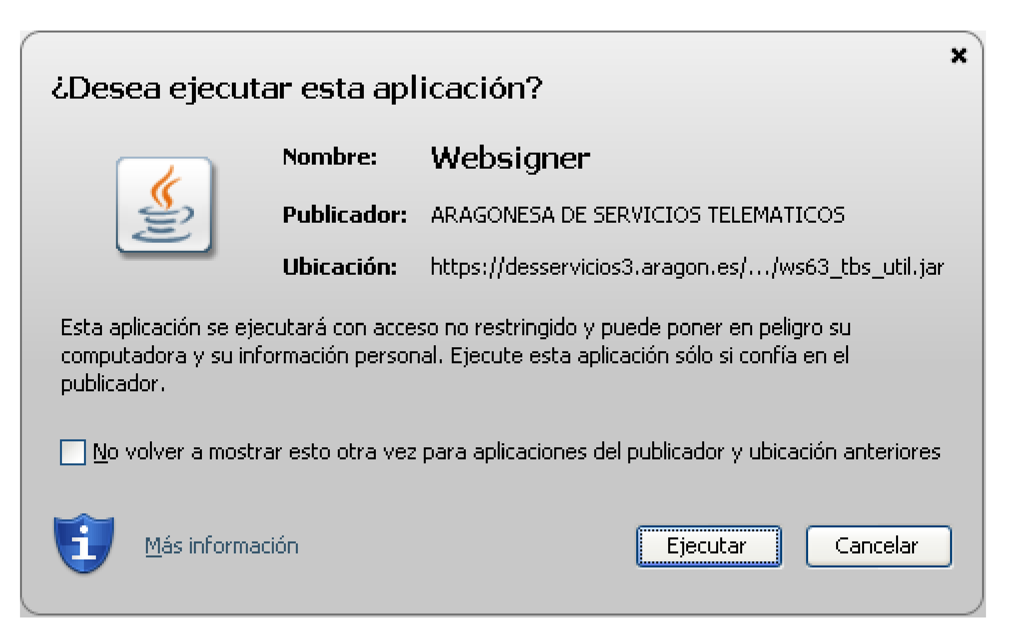
4.9.2.1. Seguridad Alta

Las pruebas para dicha versión se han realizado con la siguiente configuración de seguridad de Java:





Se indica Más Tarde para continuar con la instalación con esta configuración.



Al Ejecutar, se queda bloqueado, indicando el siguiente error en la consola de java:

security: LiveConnect (JavaScript) blocked due to security settings.

Este error se soluciona a partir de la versión v1.7.0_51 de Java.

4.9.2.2. Seguridad Media

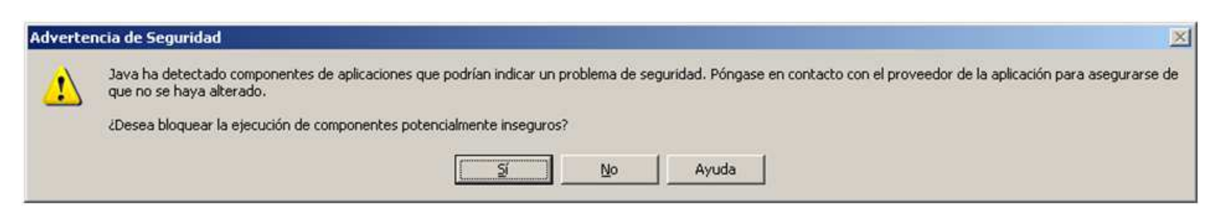
Las pruebas para dicha versión se han realizado con la siguiente configuración de seguridad de Java:



,



Al Ejecutar, se muestra un nuevo mensaje.



Habría que indicar No, para que la seguridad, no bloquee la instalación de WebSigner.

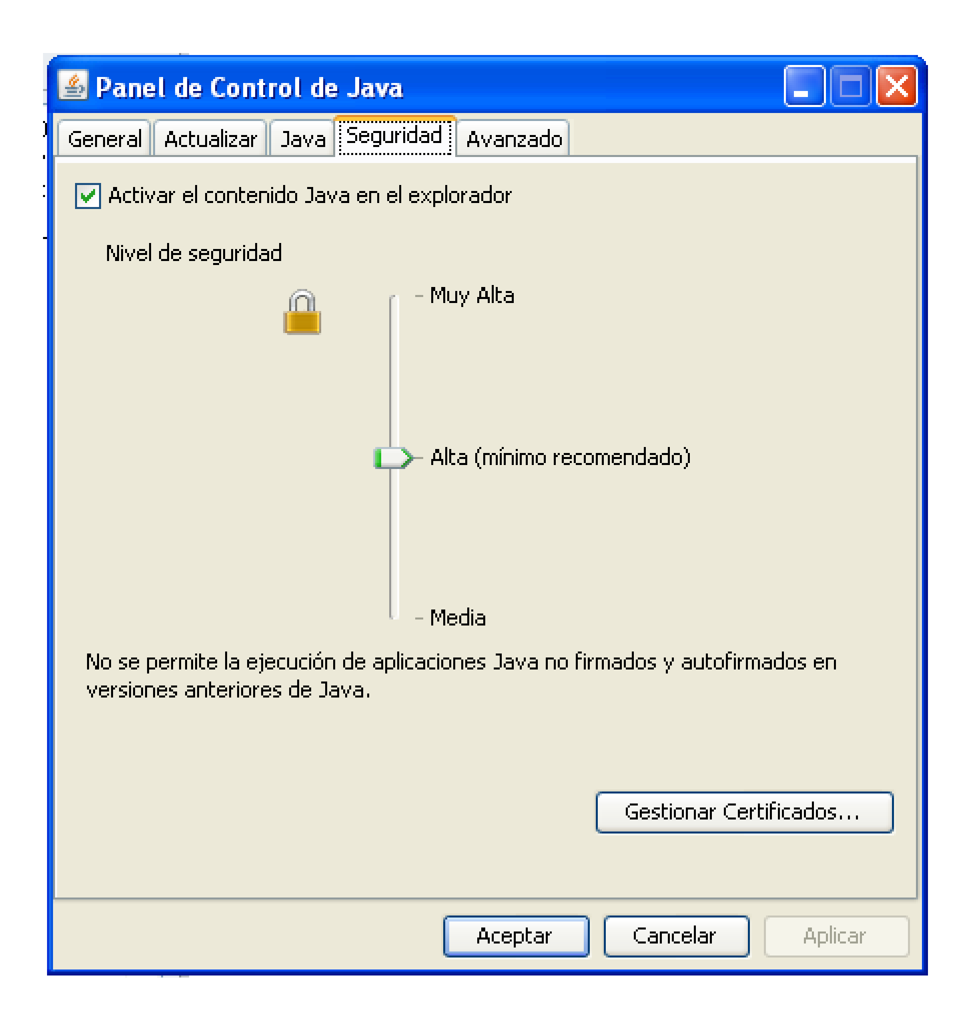


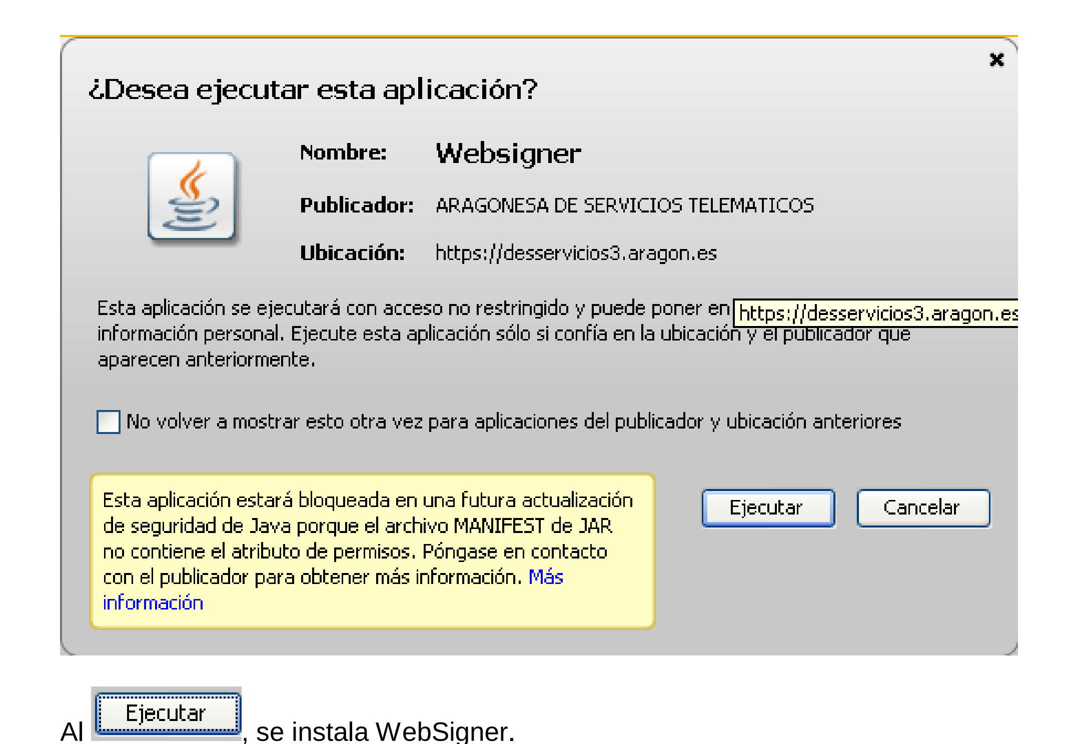
4.9.3. Java 1.7.0.51

A partir de la versión v1.7.0_51, se solucionan los problemas de bloqueo identificados en la versión anterior.

4.9.3.1. Seguridad Alta

Las pruebas para dicha versión se han realizado con la siguiente configuración de seguridad de Java:





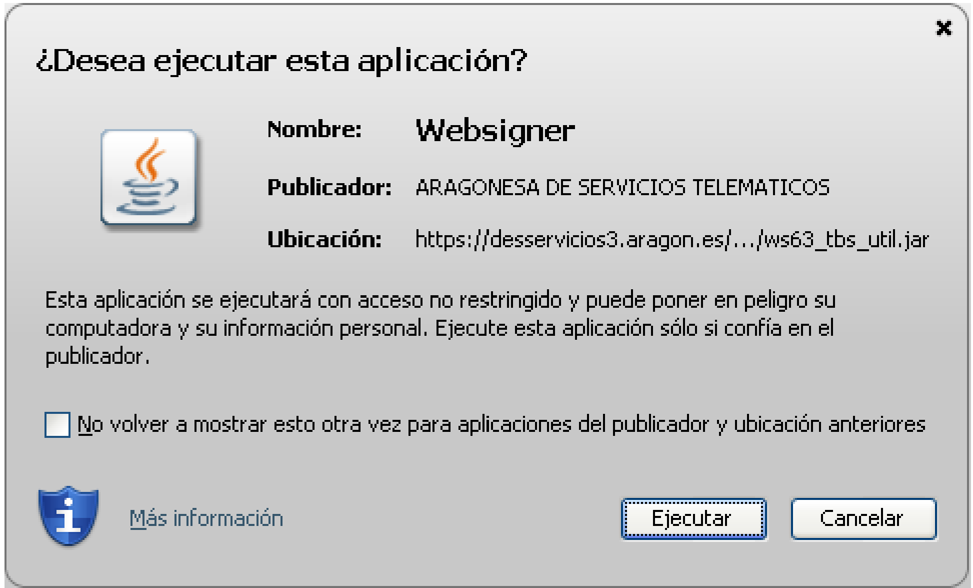
Al [Ejecutar], se instala WebSigner.

4.9.3.2. Seguridad Media

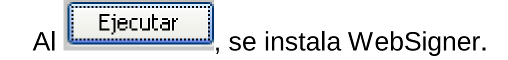
Las pruebas para dicha versión se han realizado con la siguiente configuración de seguridad de Java:



,



Entidad Pública Aragonesa de Servicios Telemáticos
Pº María Agustín 25-27-29 • 50071 ZARAGOZA
Tel. 976 71 4495 • Fax. 976 71 4395
www.aragon.es

Al 

, se instala WebSigner.